Attacks on Authentication: States enter the threat landscape

Phillip Hallam-Baker
Comodo Group Inc.

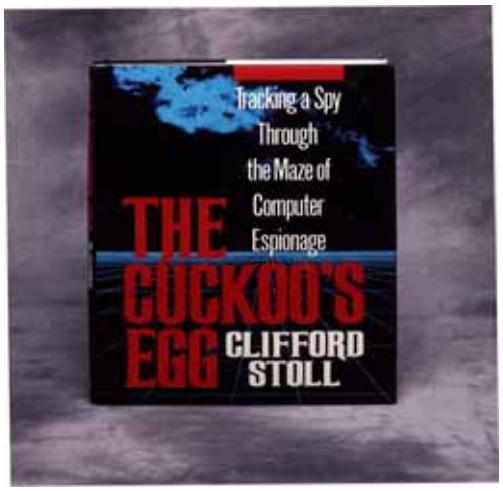
An attack is an attack

- Who cares who caused your system breach?
  - Bored teen
  - Organized crime
  - Terrorists
  - State agency

State attacks differ because

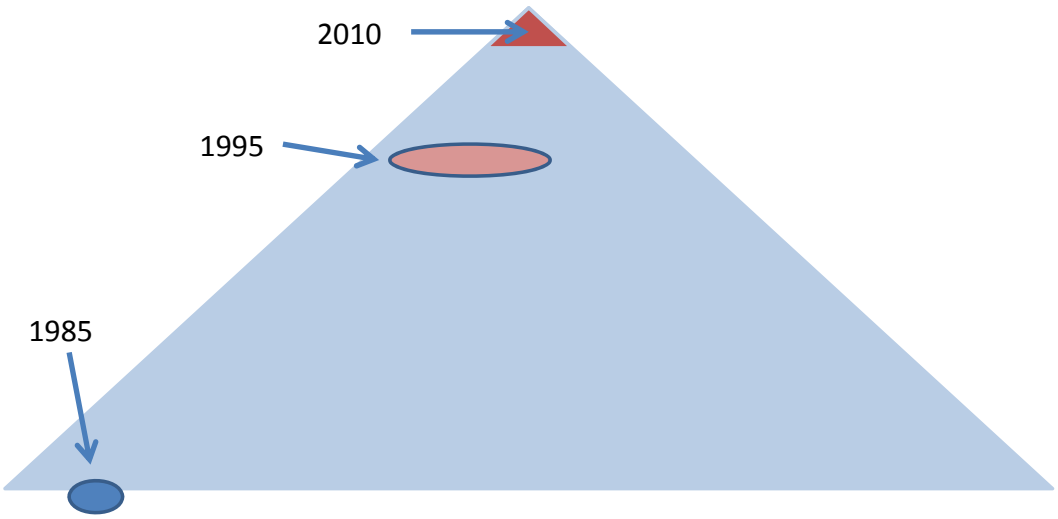
- Motive
  - Driven by politics, not profit
  - Raising cost of attack is not a winning strategy
- Resources
  - More of everything (people, knowledge, cash)
- Sovereign immunity

Is this New?



- 1986
  - 1200 baud modem
- Hacked US military
  - Dockmaster
- Results sold to KGB

What has changed



Cyber Treaties

- Shanghai Cooperation Organization (SCO)
  - Founded 2001
  - Russia, China, others
  - 50% of world population

2008 SCO Cyber Treaty

In the process of cooperation in accordance with this agreement the parties shall proceed from the assumption that there are the following main threats in the field of ensuring international information security:

1.Development and use of information weapons, preparations for and waging information war;

2.Information terrorism

3.Information crime

4.Use of the dominant position in the information space to the detriment of the interests and security of other states

5.Dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states

6.Natural and/or man-made threats to safe and stable operation of global and national information infrastructures

(Unofficial translation)

2008 SCO Cyber Treaty

Unofficial interpretation

In the process of cooperation in accordance with this agreement the parties shall proceed from the assumption that there are the following main threats in the field of ensuring international information security:

1.Development and use of information weapons, preparations for and waging information war; **Information Engagement**

2.Information terrorism **Freedom of Speech**

3.Information crime **Strikes, demonstrations, protests**

4.Use of the dominant position in the information space to the detriment of the interests and security of other states **The US, Microsoft, Google**

5.Dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states **Falun Gong**

6.Natural and/or man-made threats to safe and stable operation of global and national information infrastructures **Cyber Security**

(Unofficial translation)

2011 Attacks on PKI

- Complacency
- Inapplicable Controls
- Unenforced controls
- Inapplicable Audits
- Risk concentration

Attack Timeline

- June 2010 StuxNet malware
- Dec 2010 Arab Spring begins
- March 2011 Comodo Reseller Mis-Issue
- March 2011 RSA Breach
- May 2011 Syrian Interception Attempt
- July 2011 DigiNotar Breach

Attack Hierarchy

- Subject defaults after valid issue
  - What revocation was designed to prevent
- Unintentional mis-issue
  - Revocation / Recall
- CA Breach
  - Policy & Audit, Root revocation
- Intentional mis-issue / CA Fraud
  - Transparency, Root revocation

StuxNet

- Sophisticated
  - Four zero day attacks
    - Almost certainly a state actor, (US or Russia)
  - Used two code signing certificates
- Is believed to have targeted Iran
  - 30% drop in uranium enrichment at Natanz
  - Payload configuration matches IAEA parameters

Comodo Reseller Mis-Issue

- March 15 A Comodo Reseller was breached
  - Did not have an intermediate cert
  - Was authorized to perform validation checks
  - Attacker requested issue of 9 certificates
  - Reseller detected anomalous request
    - Alerted Comodo
    - All 9 Certificates were revoked

Some details

- Attack originated from an Iranian IP address
- Attacker sent emails after attack
  - Complained about attack being made public
  - Attempted to lay a false trail

PR Offensive

- Pastebin responsibility claim 11 days later
  - Completely different style of writing
  - Appears to be a braggart (looks intentional)
  - Makes untrue claims
    - Alleged breach of a competitor CA
  - Recites regime propaganda
  - Denies the regime is behind the attack
  - Affirms that the regime was to use the certificates

Syrian Interception Attempt

- 12 May 2012: Facebook traffic intercepted
  - Attributed to Syrian Telecoms ministry (EFF)
  - Not a sophisticated effort
    - Did not use a CA issued cert
    - Caused warnings to pop up

DigiNotar Breach

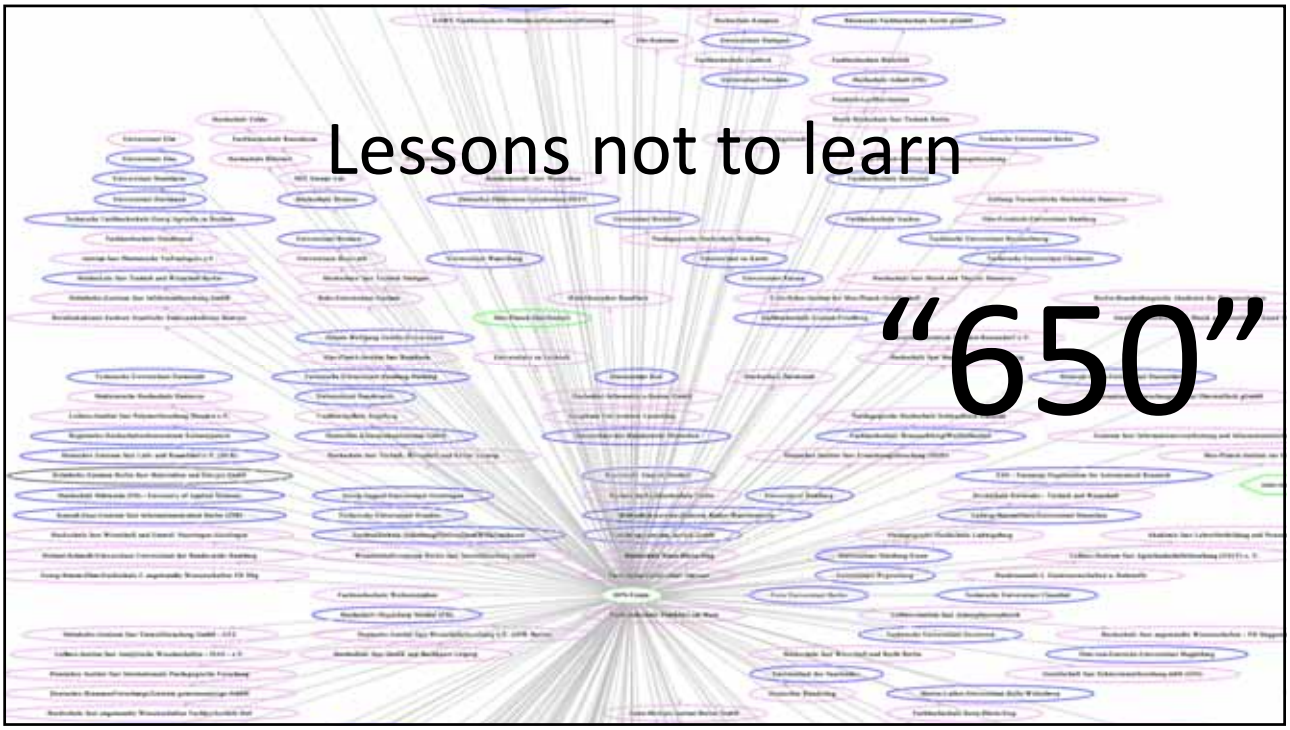
- 10 July 2011 CA Breached
  - Attacker gained full control of HSMs, audit logs
  - Fraudulent wildcard certificates issued
  - Local records deleted
- 19 July 2011 CA detected breach
- 29 Aug 2011 Google detected certificates
  - Chrome checks google.com certificates

DigiNotar Lessons

- DigiNotar had a CA audit
  - It was for a completely different CA
  - The auditor did not check the SSL CA
  - Audit was accepted by browsers as valid
- Certificate validation protocol is broken
  - CA reported status 'good' for certs it should have known it never issued
- System lacks transparency
  - CA knew it was breached but did not report

RSA Breach

- 17 March 2011
  - SecureID two factor authentication compromised
  - Attack on RSA apparently a means to attack others
  - ‘Linked to’ China
    - Tool used was written in China
    - Command and control hosted in China



Lets be fair

CA Breaches

- In 20 years
  - 2 Mis-issue events
  - 1 Breach

Software Vulnerabilities

- Buffer over-run
- Integer overflow
- Privilege escalation

DNS name hijacking

Lessons to learn

Complacency

- SSL/TLS was designed to mitigate commercial risk
  - Its only money
  - Usability is a higher priority than absolute security
  - Most browsers will accept revoked certificates
    - Cert is accepted when OCSP service is not available
  - SSL/TLS is not a user authentication protocol
    - Requires the password be disclosed for verification

‘An attack on one is an attack on all’

- The industry has changed
  - Information exchanges share threat reports
  - Share network security expertise
    - Crown jewels put on the table
  - New approaches to revocation
  - New approaches to PKI

CA/Browser Forum

- Originally established to develop EV guidelines
  - Since expanded scope to all CA issued SSL certs
- Now changing:
  - Open & Transparent
  - Information exchange
  - (TBS)

Problems with Audits

- Comodo
  - Audit failed to determine a reseller held RA rights
  - Policy did not require RA to be covered by audit
- DigiNotar
  - CA held a qualifying audit
  - But that audit applied to a different system

- New CABForum requirement (in progress):
  - Audit must cover all parts of the system that can authorize certificate issue

Transparency Trumps Audit

- Google Proposal: Certificate Transparency
  - Allow 3rd parties to verify compliance
  - No access to private information required
- A state actor can subvert an audit
  - Use coertion
  - Transparency resists subversion

Changing the model

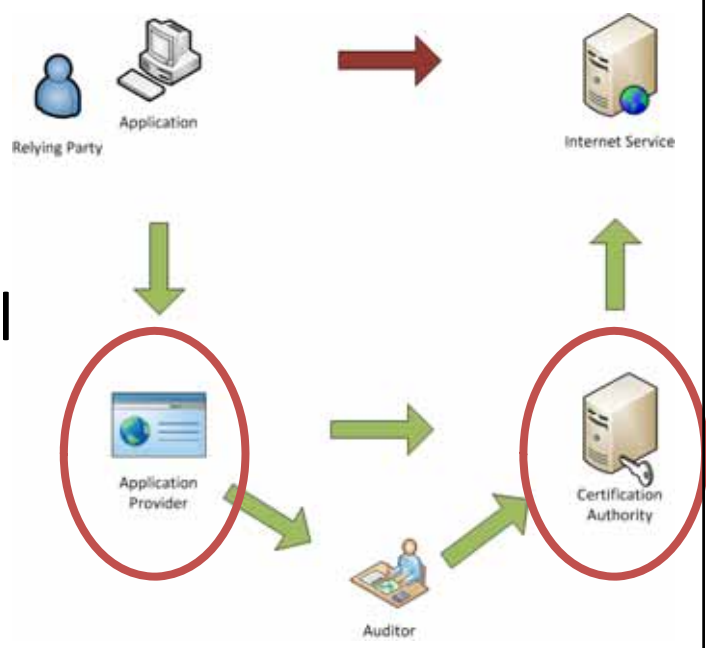
- Ideas are easy
- The real problem is change
  - Internet has 2 billion users
    - Change takes time
      - DNSSEC, 15 years and counting
      - IPv6 15 years and counting

Deployment Deadlock

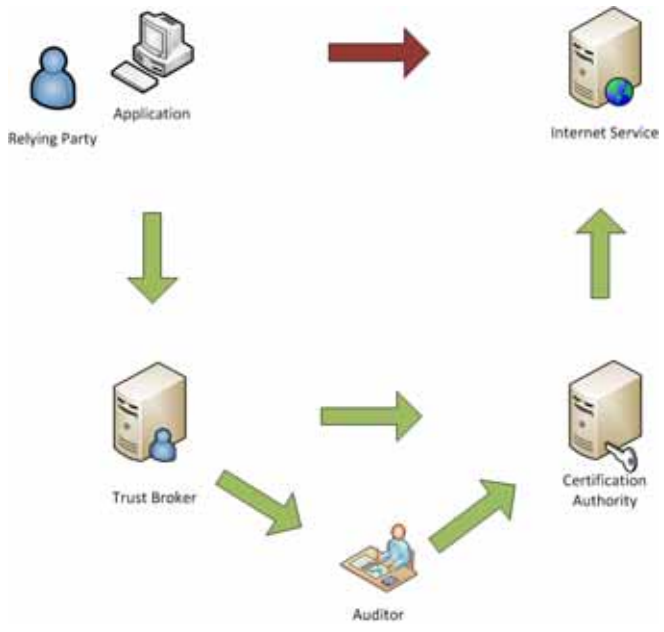
- Can't deploy a new trust service without clients that will consume it
- Can't deploy clients without a service to use

- Break the deadlock

Change the Model



Change the Model



Trust Broker

- AntiVirus for Certificates
  - Chosen by user to suit their needs
  - A dependable revocation service
  - Credible threat
    - Drop bad certificates

CertSentry

- Starting point for Trust broker
  - Deployed in Comodo Dragon 18
- Next generation: Omnibroker

Conclusions

- State actors must be considered a threat
  - Attacks are rare but consequential
  - Old assumptions of risk are obsolete
- The Internet trust infrastructure needs work
  - But any new proposal must meet *all* the requirements of the old